Amendments to the Specification

Please replace the paragraph that begins on Page1, line 5 and carries over to Page 2, line 4 with the following marked-up replacement paragraph:

-- The present invention is related to the following commonly-assigned U. S. Patents: U. S. Patent 7,010,681 (serial ~~Patents: _____ (serial~~ number 09/240,387, filed 01/29/1999), titled "Method, System and Apparatus for Selecting Encryption Levels Based on Policy Profiling"; U. S. Patent 6,585,778 (serial number 09/385,899, filed 08/30/1999), titled "Enforcing Data Policy Using Style Sheet ~~Processing"; _____ (serial~~ Processing"; U. S. Patent 6,931,532 (serial number 09/422,430, filed 10/21/1999), titled "Selective Data Encryption Using Style Sheet ~~Processing"; _____ (serial~~ Processing"; U. S. Patent 6,961,849 (serial number 09/422,537, filed 10/21/1999), titled "Selective Data Encryption Using Style Sheet Processing for Decryption by a Client ~~Proxy"; _____ (serial~~ Proxy"; U. S. Patent 6,978,367 (serial number 09/422,492, filed 10/21/1999), titled "Selective Data Encryption Using Style Sheet Processing for Decryption by a Group ~~Clerk"; _____ (serial~~ Clerk"; U. S. Patent 6,941,459 (serial number 09/422,431, filed 10/21/1999), titled "Selective Data Encryption Using Style Sheet Processing for Decryption by a Key Recovery Agent"; and _____ (serial number 10/455,068, filed 6/5/2003), titled "Method, System and Program Product for Limiting Insertion of Content between Computer Programs". --

Please replace the paragraph on Page 21, lines 5 - 11 with the following marked-up replacement paragraph:

-- On the other hand, the security container itself has some methods and properties of its own, and thus the intercepted invocation may refer to one of these rather than to the document

component object 230. The interface 210 to the security container preferably includes, for example, one or more methods for managing access to the contained object. Thus, a method referred to as "manage access", depicted at 211, might be used by an administrator or other privileged user to add, change, or delete users or user groups (or processes, equivalently) in the list of authorized entities. This is represented in Fig. 2 by arrow 251. --

Please replace the paragraph that begins on Page 21, line 12 and carries over to Page 22, line 6 with the following marked-up replacement paragraph:

-- Before discussing embodiments of the present invention in further detail, several commonly-assigned inventions will first be described. Commonly-assigned U. S. Patent 7,010,681 (serial ~~Patent _____ (serial~~ number 09/240,387), titled "Method, System and Apparatus for Selecting Encryption Levels Based on Policy Profiling", teaches techniques that operate with documents having multiple levels of security for sections of their contained content. When a user requests a document, the user's access rights are determined, and any document sections for which this user's access rights are insufficient will be "filtered out", i.e., deleted from the document version provided to that user. In addition or instead, the filtering may be based on information such as whether the user's device is sufficiently secure to receive various sections of the document or whether the device is capable of decrypting the content, once received. The sections not filtered out of the document are then encrypted, using an encryption technique selected using a policy profile that is adapted to variable security levels. This is distinct from the present invention, which provides an identical document component, protected within an identical security container, to all recipients and does not conditionally modify a document for different

users, as in the commonly-assigned invention. --

Please replace the paragraph on Page 22, lines 7 - 16 with the following marked-up replacement paragraph:

-- Commonly-assigned U. S. Patent 6,585,778 (serial number 09/385,399), titled "Enforcing Data Policy Using Style Sheet Processing", teaches techniques whereby the content of a document is controlled using stored policy information. Stored "policy objects" are disclosed, where these policy objects are referenced in the schema or Document Type Definition ("DTD") that defines allowable document syntax. As an example of using a policy object for enforcing data policy, the context of a user who requests a document can be determined, and a policy object can evaluate whether selected portions of that document should be delivered to the user, given his current context. Extensions to these policy objects are defined in commonly-assigned U. S. ~~Patent _____ (serial~~ Patent 6,931,532 (serial number 09/422,430), which is titled "Selective Data Encryption Using Style Sheet Processing" (hereinafter, "the selective data encryption invention"). --

Please replace the paragraph that begins on Page 23, line 16 and carries over to Page 24, line 5 with the following marked-up replacement paragraph:

-- Alternative approaches for performing the decryption of a document that has been selectively encrypted according to the selective data encryption invention are disclosed in commonly-assigned U. S. Patent 6,961,849 (serial ~~Patent _____ (serial~~ number 09/422,537), titled "Selective Data Encryption Using Style Sheet Processing for Decryption by a Client Proxy",

U. S. Patent 6,978,367 (serial ~~Patent _____ (serial~~ number 09/422,492), titled "Selective Data Encryption Using Style Sheet Processing for Decryption by a Group Clerk", and U. S. Patent 6,941,459 (serial ~~Patent _____ (serial~~ number 09/422,431), titled "Selective Data Encryption Using Style Sheet Processing for Decryption by a Key Recovery Agent". These commonly-assigned inventions, in addition to the selective data encryption invention, are referred to hereinafter as "the referenced inventions", and are hereby incorporated herein by reference as if set forth fully. --

Please replace the paragraph on Page 25, lines 1 - 7 with the following marked-up replacement paragraph:

-- As shown in the diagram of Fig. 3A, each key class 300 includes an identification of its encryption algorithm (element 310), its key length (element 320), zero or more hints for use with the algorithm (element 330), a DN of the component creator (element [[350]] 340), an X.509 certificate of the component creator or an identifier of this X.509 certificate (element [[360]] 350), and one or more key objects (elements 360, 370, ... 390). In preferred embodiments, key class 300 is used as the encryption header 110 of Fig. 1. Accordingly, references to a key class or to an encryption header are used interchangeably herein. --

Please replace the paragraph on Page 29, lines 8 - 16 with the following marked-up replacement paragraph:

-- In the case of a group, the DN identifies the group. Individuals who are members of the group use techniques outside the scope of the present invention to obtain the group's private

key or request that it be employed on their behalf. Commonly-assigned U. S. ~~Patent~~ ~~(serial~~ Patent 6,978,367 (serial number 09/422,492), titled "Selective Data Encryption Using Style Sheet Processing for Decryption by a Group Clerk", defines one way to accomplish this. (The public key in the X.509 certificate may therefore belong to a group that is identified in the "subject" field 440, while the DN belongs to the group clerk.) However, other techniques may be used for determining a group's membership and utilizing the group's private key on behalf of individual group members, without deviating from the scope of the present invention. --

Please replace the paragraph that begins on Page 29, line 17 and carries over to Page 30, line 1 with the following marked-up replacement paragraph:

-- The manner in which the encryption algorithm and key length are selected, and in which the value of the symmetric key is determined, does not form part of the present invention. One way in which the algorithm and key length may be selected is described in commonly-assigned U. S. ~~Patent~~ ~~(serial~~ Patent 7,010,681 (serial number 09/240,387), "Method, System and Apparatus for Selecting Encryption Levels Based on Policy Profiling". --

Please replace the paragraph that begins on Page 30, line 14 and carries over to Page 31, line 13 with the following marked-up replacement paragraph:

-- A sample employee record 600 is provided in Fig. 6, using XML format. The current salary and medical information for this employee (encoded with the "curr_salary" and ~~"medical"~~ "medical_condition" elements, respectively) may be considered sensitive or confidential information, thereby necessitating controls over access to the employee record, and controls on

the functions that can be performed on that record. These access and functional controls may be provided by the present invention's security container. Fig. 7 shows, conceptually, how the security container represents the employee record 600 to a user or process that has not yet been authenticated. In other words, the document component 600 from Fig. 6 is stored in the security container in encrypted, unintelligible form, denoted generally by element 750 of Fig. 7. The encryption header 710 of security container 700 contains, in this example, the key class 301 from Fig. 3B. Security container 700 also contains a set of encrypted rules (denoted generally by element 720), a secure hash (denoted at element 730) that has been created over these rules, and a digital signature 740 that has been created over the key class 710 and the rules. As has been described with reference to the example in Fig. 3B, key class 301 contains key elements for three different sets of users (including two groups of users and one individual user). Thus, any user who is in either of the groups, or who is the specified individual user, has at least some access rights to the information in security container 700. Software acting on the user's behalf can quickly determine, by scanning the non-encrypted DN portions of the key classes, whether to proceed with attempting decryption of the encrypted elements (i.e., the encrypted symmetric key specified as the value of the corresponding "Ekey" attribute) using an associated private key. --

Please replace the paragraph that begins on Page 39, line 18 and carries over to Page 41, line 1 with the following marked-up replacement paragraph:

-- As an alternative to a user decrypting the rules and content with his own private key, or a group clerk decrypting the rules and content on behalf of group members, the decryption may be carried out by a client proxy that operates on behalf of the client, or by a key recovery agent that

effectively operates as an authorized user of all secured content. Techniques for using key class information with a client proxy and key recovery agent are disclosed in detail in the referenced inventions (and in particular, in U. S. Patents 6,961,849. serial ~~Patents _____, serial~~ number 09/422,537, and 6,941,459, serial ~~and _____, serial~~ number 09/422,431). Generally, communications between the client and client proxy use a mutually-authenticated secure channel, if possible, so that the client proxy can decrypt information and return it in clear text form to the client. Alternatively, the client proxy can re-encrypt information with the client's public key (or with a symmetric key shared between the client and the proxy) to securely return the information in the absence of a mutually-authenticated secure channel. Note that, in preferred embodiments, the client proxy must be an authorized user of the security container in order to access the container on behalf of the client. In the case of a key recovery agent, it may be necessary to recover encrypted document components for tracking purposes, for auditing, when the only other authorized user loses his access rights, and so forth. As disclosed in the referenced inventions, a key recovery agent can recover the clear text value of any symmetric key by having a key object defined, within each key class, for the key recovery agent. If more than one key recovery agent is allowed, then the key object can be defined as identifying a group. The key recovery agent is preferably permitted to bypass the rules filtering (e.g., by using a special ID in the rules, where this ID is associated with the key recovery agent), so it can always access all methods and properties of the embedded document component. The key recovery agent also preferably has access to any rules defined for managing the security container (as illustrated generally at 211 in Fig. 2). In any case, the key recovery process for a client proxy or a key recovery agent proceeds as has been described above with reference to Fig. 8. --